In the claims:

All of the claims standing for examination are reproduced below with appropriate status indication.

Cancel claims 1-28.

29. (New) A wireless database management system, comprising:

first virtual private network (VPN) management software operating on at least one server providing Internet access to client-held wireless communication appliances, the VPN software limiting access to a subset of the wireless communication appliances that subscribe to the VPN; and

second VPN management software operating on at least one server with access to the Internet and providing access to one or more databases associated with the subscribing subset of wireless communication devices;

wherein operation of the first and second VPN management software creates a VPN tunnel in the Internet restricted to data addressed to or from the subscribing subset of wireless communication appliances.

30. (New) The wireless database management system of claim 29 wherein the wireless communication appliances are one of a personal digital assistant (PDA), cell phone, two-way pager or other similar device.

31. (New) The wireless database management system of claim 29 wherein the first virtual private network (VPN) management software operating on at least one server providing Internet access to client-held wireless communication appliances is a VPN-controlled wireless proxy server securing data transferred between the client-held wireless

communication appliances and the Internet.

32. (New) The wireless database management system of claim 29, wherein the data transfers between the server providing Internet access to client-held wireless communication appliances are encrypted with a public key method.

33. (New) The wireless database management system of claim 29, wherein the data transfers between the server with access to the Internet and providing access to one or more databases associated with the subscribing subset of wireless communication devices are encrypted with a private key method.

34. (New) The wireless database management system of claim 29, wherein users of the wireless communication appliances are authenticated before allowing access to the databases.

35. (New) The wireless database management system of claim 29, wherein software implemented on the server with access to the Internet and providing access to one or more databases sets an adjustable timeout for connections between the wireless communication appliances and the server.

36. (New) The wireless database management system of claim 35, wherein the server identifies a session between the wireless communication appliances and the server with a session identification phrase, and storing the session identification phrase in memory.

37. (New) The wireless database management system of claim 29, wherein a firewall is implemented between the Internet and the server connected to the databases, thereby limiting access to IP addresses of the wireless communication devices.

38. (New) The wireless database management system of claim 37, wherein a second

firewall is implemented between the server and the databases.

39. (New) A method for securing data transfers in a wireless database management system, comprising steps of:

a) providing first virtual private network (VPN) management software operating on at least one server providing Internet access to client-held wireless communication appliances, the VPN software limiting access to a subset of the wireless communication appliances that subscribe to the VPN; and

b) providing a second VPN management software operating on at least one server with access to the Internet and providing access to one or more databases associated with the subscribing subset of wireless communication devices; and

c) operating the first and second VPN management software creating a VPN tunnel in the Internet restricted to data addressed to or from the subscribing subset of wireless communication appliances.

40. (New) The method of claim 39, wherein the wireless communication appliances are one of a personal digital assistant (PDA), cell phone, two-way pager or other similar device.

41. (New) The method of claim 39 wherein in step a), the first virtual private network (VPN) management software operating on at least one server providing Internet access to client-held wireless communication appliances is a VPN-controlled wireless proxy server securing data transferred between the client-held wireless communication appliances and the Internet.

42. (New) The method of claim 39 wherein in step a) the data transfers between the server providing Internet access to client-held wireless communication appliances are encrypted with a public key method.

43. (New) The method of claim 39 wherein in step b), the data transfers between the server with access to the Internet and providing access to one or more databases associated with the subscribing subset of wireless communication devices are encrypted with a private key method.

44. (New) The method of claim 39, further providing a step of authenticating users of the wireless communication appliances before allowing access to the databases.

45. (New) The method of claim 39 wherein in step b) an adjustable timeout is provided for connections between the wireless communication appliances and the server.

46. (New) The method of claim 39, further providing a step for identifying a session between the server and the wireless communication appliances of step a) with a session identification phrase, and storing the session identification phrase in memory.

47. (New) The method of claim 39 wherein in step b) a firewall is provided between the Internet and the server connected to the databases, thereby limiting access to IP addresses of the wireless communication devices.

48. (New) The method of claim 47 wherein a second firewall is implemented between the server and the databases.